Beweis einer Vandiver'schen Vermutung bezüglich des zweiten Falles des letzten Fermat'schen Satzes.

Von PETER DÉNES in Budapest.

Es seien p eine ungerade Primzahl, $\Omega(\zeta)$ der Kreiskörper der p-ten Einheitswurzeln, $\zeta = e^{2\pi i/p}$, $\lambda = 1-\zeta$, $\mathfrak{l} = [\lambda]$, $\Lambda = (1-\zeta)(1-\zeta^{-1})$, ε_0 eine Einheit in $\Omega(\zeta)$.

VANDIVER[1]) bewies den folgenden Satz: *Unter den Bedingungen:*

1°. *Der zweite Faktor der Klassenzahl von $\Omega(\zeta)$ ist nicht durch p teilbar;*

2°. *Keiner der Bernoullischen Zahlen $B_{n,p}\left(n = 1,\ldots,\frac{p-3}{2}\right)$ ist durch p^3 teilbar;*

ist die Fermat'sche Gleichung im zweiten Fall

$$\xi^p + \eta^p = \varepsilon_0 \cdot \Lambda^{mp} \psi^p \tag{1}$$

mit nicht verschwindenden, relativ primen Zahlen ξ, η, ψ des reellen Unterkörpers $\Omega(\zeta+\zeta^{-1})$ von $\Omega(\zeta)$ unlösbar.

In einer späteren Arbeit gab VANDIVER[2]) seiner Ansicht Ausdruck, daß *die Bedingung der Teilerfremdheit der Zahlen ξ, η, ψ im obigen Satz weglassen werden kann*, er bewies jedoch diese Vermutung nicht.

In der vorliegenden Arbeit wollen wir diese Vandiver'sche Vermutung beweisen.

Es soll also angenommen werden, daß die Zahlen ξ, η keinen gemeinsamen Zahlenfaktor, aber den gemeinsamen Idealfaktor $\mathfrak{d}$ als größten gemeinsamen Teiler besitzen:

$$[\xi, \eta] = \mathfrak{d};$$

$\mathfrak{d}$ ist ein Ideal des Unterkörpers $\Omega(\zeta+\zeta^{-1})$.

Die Gleichung (1) zerfällt in die bekannten Faktoren:

$$\begin{cases} \xi + \eta = \mathfrak{l}^{2mp-p+1}\mathfrak{j}_0^p\mathfrak{d} \\ \xi + \eta\zeta^i = \mathfrak{l}\mathfrak{j}_i^p\mathfrak{d} \qquad (i = 1, 2, \ldots, p-1), \end{cases} \tag{2}$$

[1]) H. S. VANDIVER, On Fermat's last theorem, *Transactions American Math. Soc.*, **31** (1929), pp. 613—642.

[2]) H. S. VANDIVER, Summary of results and proofs on Fermat's last theorem, V, *Proceedings National Acad. Sci. USA*, **16** (1930), pp. 298—304.

in welchen $\mathfrak{j}_0, \mathfrak{j}_1, \ldots, \mathfrak{j}_{p-1}$ zueinander und zu $\mathfrak{l}$ prime Ideale in $\Omega(\zeta)$ sind. Hätten nämlich etwa $\mathfrak{j}_i$ und $\mathfrak{j}_k$ das von dem Einheitsideal verschiedene Ideal $\mathfrak{a}$ als gemeinsamen Faktor, so erhalten wir aus der Differenz der i-ten und k-ten Gleichung in (2), daß auch

$$\frac{\xi}{\mathfrak{d}} \quad \text{und} \quad \frac{\eta}{\mathfrak{d}}$$

durch $\mathfrak{a}$ teilbar sein müßten; dies ist jedoch unmöglich, da $\frac{\xi}{\mathfrak{d}}$ und $\frac{\eta}{\mathfrak{d}}$ relativ prim sind.

Es bestehen mit Rücksicht auf die erste Gleichung in (2) die folgenden Kongruenzen:

$$\frac{\xi+\eta\zeta^i}{1-\zeta^i} = \frac{\xi+\eta}{1-\zeta^i} - \eta \equiv -\eta \pmod{\mathfrak{l}^p} \qquad (i=1,2,\ldots,p-1).$$

Bedeuten i und k zwei beliebige Zahlen aus $1, 2, \ldots, p-1$ und a eine positive ganze Zahl, $a \leqq p$, so ist

$$\left(\frac{\xi+\eta\zeta^i}{1-\zeta^i}\right)^a \left(\frac{\xi+\eta\zeta^k}{1-\zeta^k}\right)^{p-a} \equiv -\eta^p \pmod{\mathfrak{l}^p}. \tag{3}$$

Aus (2) und (3) folgt, daß das Hauptideal

$$\mathfrak{j}_i^{ap}\,\mathfrak{j}_k^{(p-a)p}\,\mathfrak{d}^p \qquad (i,k=1,2,\ldots,p-1)$$

einer primären Zahl in $\Omega(\zeta)$ gleich ist[3]). Gemäß Lemma 1 der zitierten Arbeit von Vandiver[1]) ist ein Ideal, dessen p-te Potenz eine primäre Zahl ist, selbst ein Hauptideal, falls der zweite Faktor der Klassenzahl von $\Omega(\zeta)$ prim zu p ist:

$$\mathfrak{j}_i^{a}\,\mathfrak{j}_k^{p-a}\,\mathfrak{d} \sim 1 \qquad (i,k=1,2,\ldots,p-1). \tag{4}$$

Zufolge der Gleichungen (2) gilt außerdem

$$\mathfrak{j}_k^{p}\,\mathfrak{d} \sim 1 \qquad (k=1,2,\ldots,p-1) \tag{5}$$

und wenn man in (4) $a=1$ setzt, ergibt sich aus (4) und (5):

$$\mathfrak{j}_i \sim \mathfrak{j}_k \qquad (i,k=1,2,\ldots,p-1). \tag{6}$$

Wir nehmen jetzt in Betracht, daß nach (1), (2)

$$[\psi] = \mathfrak{d} \prod_{i=0}^{p-1} \mathfrak{j}_i \sim 1 \tag{7}$$

ist, woraus wegen (5) und (6)

$$\mathfrak{j}_0 \sim \mathfrak{j}_k \qquad (k=1,2,\ldots,p-1) \tag{8}$$

folgt. $\mathfrak{j}_0$ ist zufolge (2) reell, gehört also zu einer Idealklasse C_0 des Körpers $\Omega(\zeta+\zeta^{-1})$. Ist $\mathfrak{t}$ ein reelles Ideal der Klasse C_0^{-1}, welches keinen Hauptidealteiler

[3]) Eine Zahl α des Körpers $\Omega(\zeta)$ heißt primär, wenn es eine Zahl β im $\Omega(\zeta)$ gibt, welche die Kongruenz $\alpha \equiv \beta^p \pmod{\mathfrak{l}^p}$ erfüllt.

besitzt, so sind zufolge (8) die $\mathfrak{t}\mathfrak{j}_k$ Hauptideale in $\Omega(\zeta)$:

$$[\varrho_k] = \mathfrak{t}\mathfrak{j}_k \qquad (k = 0, 1, \ldots, p-1). \tag{9}$$

Die $\varrho_0, \varrho_1, \ldots, \varrho_{p-1}$ bezeichnen zahlenteilerfremde Zahlen des Körpers $\Omega(\zeta)$, welche Eigenschaft daraus folgt, daß die Ideale $\mathfrak{j}_0, \mathfrak{j}_1, \ldots, \mathfrak{j}_{p-1}$ relativ prim sind und $\mathfrak{t}$ keinen Hauptidealteiler besitzt.

Nach der Definition kann ϱ_0 reell angenommen werden, dagegen kann man die Zahlen ϱ_k und ϱ_{p-k} $\left(k = 1, 2, \ldots, \frac{p-1}{2}\right)$ konjugiert imaginär wählen.

Bezeichnet k eine von $0, i$ und $p-i$ verschiedene Zahl, $k, i < p$, so können wir aus (2) mittels (9) die folgenden drei Gleichungen bilden:

$$\left\{\begin{aligned} &\frac{\xi+\eta}{\xi+\eta\zeta^k} = \beta_0 \lambda^{(2m-1)p} \frac{\varrho_0^p}{\varrho_k^p}, \\ &\frac{\xi+\eta\zeta^i}{\xi+\eta\zeta^k} = \beta_i \frac{\varrho_i^p}{\varrho_k^p}, \\ &\frac{\xi+\eta\zeta^{-i}}{\xi+\eta\zeta^k} = \beta_{p-i} \frac{\varrho_{p-i}^p}{\varrho_k^p}, \end{aligned}\right. \tag{10}$$

wo $\beta_0, \beta_i, \beta_{p-i}$ Einheiten in $\Omega(\zeta)$ sind. Aus diesen folgt

$$\varrho_i^p - \vartheta_i \varrho_{p-i}^p = \vartheta_0 \lambda^{(2m-1)p} \varrho_0^p \tag{11}$$

mit den Einheiten

$$\vartheta_0 = (1+\zeta^i)\frac{\beta_0}{\beta_i},$$

$$\vartheta_i = -\zeta^i \frac{\beta_{p-i}}{\beta_i} = \frac{\xi+\eta\zeta^{-i}}{1-\zeta^{-i}} \frac{1-\zeta^i}{\xi+\eta\zeta^i} \frac{\varrho_i^p}{\varrho_{p-i}^p}. \tag{12}$$

Wir zeigen jetzt, daß $\vartheta_i = 1$ ist. Wird die Gleichung (12) als eine Kongruenz nach dem Modul $\mathfrak{l}^p$ untersucht, so ergibt sich ϑ_i primär. Da eine Einheit des Körpers $\Omega(\zeta)$ das Produkt einer reellen Einheit und einer Einheitswurzel ist, ist jede primäre Einheit in $\Omega(\zeta)$ reell. Demzufolge erzeugt die Substitution $(s = \zeta : \zeta^{-1})$ aus (11) die Gleichung

$$\varrho_{p-i}^p - \vartheta_i \varrho_i^p = -\vartheta_0 \lambda^{(2m-1)p} \varrho_0^p,$$

was mit (11) zusammen

$$\vartheta_i = 1$$

ergibt. Dann lautet (11) so:

$$\varrho_i^p - \varrho_{p-i}^p = \vartheta_0 \lambda^{(2m-1)p} \varrho_0^p, \tag{13}$$

welche Gleichung wieder in p Faktoren zerfällt:

$$\left\{\begin{aligned} &\varrho_i - \varrho_{p-i} = \mathfrak{l}^{(2m-2)p+1} \mathfrak{t}\mathfrak{g}_{i0}^p \\ &\varrho_i - \varrho_{p-i}\zeta^j = \mathfrak{l}\mathfrak{t}\mathfrak{g}_{ij}^p \end{aligned}\right. \qquad \left(\begin{aligned} &j = 1, 2, \ldots, p-1 \\ &i = 1, 2, \ldots, \frac{p-1}{2} \end{aligned}\right), \tag{14}$$

in welchen $\mathfrak{g}_{i0}, \ldots, \mathfrak{g}_{i,p-1}$ $\left(i=1,2,\ldots,\frac{p-1}{2}\right)$ zueinander und zu $\mathfrak{l}$ prime. Ideale des reellen Unterkörpers $\Omega(\zeta+\zeta^{-1})$ von $\Omega(\zeta)$ sind, weil ihre Werte sich durch Anwendung der Substitution $(s=\zeta:\zeta^{-1})$ auf die Gleichungen (14) nicht ändern.

Da ϱ_i und ϱ_{p-i} in (13) zur p-ten Potenz vorkommen, können dieselben durch Multiplikation mit einer Einheitswurzel semiprimär gemacht werden, d. h. sie sind nach dem Modul $\mathfrak{l}^2$ mit einer ganzen rationalen Zahl kongruent. Da ferner ϱ_i und ϱ_{p-i} konjugiert imaginär sind, sind sie nach $\mathfrak{l}^2$ mit derselben ganzen rationalen Zahl kongruent, also ist ihre Differenz mindenstens durch $\mathfrak{l}^2$ teilbar. Das ergibt

$$(2m-2)p+1>1,$$

d. h. $m>1$, woraus

$$\varrho_i-\varrho_{p-i}\equiv 0 \pmod{\mathfrak{l}^{2\mu+1}} \qquad \left(i=1,2,\ldots,\frac{p-1}{2}\right) \tag{15}$$

folgt.

Wegen

$$\frac{\varrho_i-\varrho_{p-i}\zeta^j}{\varrho_k-\varrho_{p-k}\zeta^j}=\frac{\mathfrak{g}_{ij}^{\mu}}{\mathfrak{g}_{kj}^{\mu}} \qquad \left(\begin{matrix} j=1,2,\ldots,p-1 \\ i,k=1,2,\ldots,\frac{p-1}{2}\end{matrix}\right),$$

sind die Ideale $\frac{\mathfrak{g}_{ij}}{\mathfrak{g}_{kj}}$ zufolge der Voraussetzung 1° Hauptideale, da dieselben reell und ihre p-te Potenzen Hauptideale sind; es gilt also für $j=1$

$$\frac{\varrho_i-\varrho_{p-i}\zeta}{\varrho_k-\varrho_{p-k}\zeta}=\delta_{ik}\frac{\varphi_i^{p}}{\varphi_k^{p}} \qquad \left(i,k=1,2,\ldots,\frac{p-1}{2}\right),$$

wo δ_{ik} Einheiten und φ_i, φ_k Zahlen in $\Omega(\zeta)$ sind, woraus wegen (15)

$$\frac{\varrho_i}{\varrho_k}\equiv\frac{\varrho_{p-i}}{\varrho_{p-k}}\equiv\delta_{ik}\frac{\varphi_i^{p}}{\varphi_k^{p}} \pmod{\mathfrak{l}^{2\mu}} \qquad \left(i,k=1,2,\ldots,\frac{p-1}{2}\right) \tag{16}$$

folgt.

Aus (10) können wir ferner die folgenden reellen Gleichungen bilden:

$$\frac{\xi^2+2\xi\eta+\eta^2}{(\xi+\eta\zeta^k)(\xi+\eta\zeta^{-k})}=\Theta_0\Lambda^{(2m-1)p}\frac{\varrho_0^{2p}}{\varrho_k^{p}\varrho_{p-k}^{p}} \tag{17}$$

$$\frac{\xi^2+\xi\eta(\zeta^i+\zeta^{-i})+\eta^2}{(\xi+\eta\zeta^k)(\xi+\eta\zeta^{-k})}=\Theta_i\frac{\varrho_i^{p}\varrho_{p-i}^{p}}{\varrho_k^{p}\varrho_{p-k}^{p}} \qquad \left(i=1,2,\ldots,\frac{p-1}{2}\right), \tag{18}$$

in welchen $\Theta_0, \Theta_1, \ldots, \Theta_{\frac{p-1}{2}}$ reelle Einheiten in $\Omega(\zeta)$ sind. Indem wir $k>2$ wählen und aus den drei Gleichungen (17) und (18) (für $i=1,2$) die Zahlen $\xi^2+\eta^2$

und $\xi\eta$ eliminieren, erhalten wir mit den Bezeichnungen $\sigma_0 = \varrho_0^2$, $\sigma_1 = \varrho_1\varrho_{p-1}$, $\sigma_2 = \varrho_2\varrho_{p-2}$ eine Gleichung

$$\sigma_1^p + e_2\sigma_2^p = e_0\Lambda^{(2m-1)p}\sigma_0^p, \tag{19}$$

wo e_0 und e_2 reelle Einheiten in $\Omega(\zeta)$ sind. Mittels (16) und (19) kann man die Kongruenz

$$e_2 \equiv -\frac{\sigma_1^p}{\sigma_2^p} \equiv -\delta_{1,2}^{2p}\frac{\varphi_1^{2p^2}}{\varphi_2^{2p^2}} \pmod{\mathfrak{l}^{2p}}$$

aufstellen und nach Lemma 2 von VANDIVER[1]) können wir folgern, daß

$$e_2 \cdot \delta_{1,2}^{-2p}$$

und demzufolge auch die Einheit e_2 die p-te Potenz einer Einheit des Körpers $\Omega(\zeta)$ ist, welche in der Gleichung (19) zur p-ten Potenz vorkommt und deshalb als eine reelle Einheit angenommen werden kann. Die Gleichung (19) gestaltet sich hierdurch

$$\sigma_1'^p + \sigma_2'^p = e_0\Lambda^{(2m-1)p}\sigma_0'^p, \tag{20}$$

wo $\sigma_0, \sigma_1, \sigma_2'$ reelle Zahlen des Körpers $\Omega(\zeta)$ sind.

Die Gleichung (20) hat dieselbe Form, wie die Gleichung (1) und da $m > 1$ war, ist auch $2m-1 > 1$. Das Ideal $\frac{[\sigma_0]}{\mathfrak{t}^2}$ besitzt dabei zufolge der Gleichungen (7) und (9) wenigere Primidealteiler, als das Ideal $\frac{[\psi]}{\mathfrak{d}}$, mit Ausnahme des Falles $\mathfrak{j}_i = 1$ $(i = 1, 2, \ldots, p-1)$.

Die Wiederholung der angewandten Methode auf die Gleichung (20) würde wieder eine zu (20) ähnliche Gleichung mit den Zahlen $\sigma_0^*, \sigma_1^*, \sigma_2^*$ ergeben, deren größter gemeinsamer Idealteiler $\mathfrak{t}^*$ ist. Das Ideal $\frac{[\sigma_0^*]}{\mathfrak{t}^*}$ kann aber wieder nur wenigere Primidealteiler haben, als das Ideal $\frac{[\sigma_0]}{\mathfrak{t}^2}$, mit Ausnahme des Falles $\mathfrak{j}_i^* = 1$ $(i = 1, 2, \ldots, p-1)$, Die Fortsetzung dieses Abstieges muß also entweder zu einem Widerspruch führen, da das Ideal $\frac{[\psi]}{\mathfrak{d}}$ nur eine endliche Anzahl von Primidealteiler besitzt, oder zu den Gleichungen

$$\sigma_1^{**} + \sigma_2^{**}\zeta^i = \mathfrak{t}^{**} \qquad (i = 1, 2, \ldots, p-1).$$

In diesem Falle ist das Ideal $\mathfrak{t}^{**}$ ein Hauptideal. Da ferner $\sigma_1^{**}, \sigma_2^{**}$ keinen gemeinsamen Zahlenteiler haben, so ist $\mathfrak{t}^{**} = 1$ und wir haben die Gleichungen

$$\frac{\sigma_1^{**} + \sigma_2^{**}\zeta^i}{1-\zeta^i} = E_i \qquad (i = 1, 2, \ldots, p-1), \tag{21}$$

wo $E_1, \ldots, E_{p-1}$ Einheiten in $\Omega(\zeta)$ sind. Weiter folgt, wie aus (2),

$$E_i \equiv -\sigma_2^{**} \pmod{\mathfrak{l}^p} \qquad (i = 1, 2, \ldots, p-1);$$

da σ_2^{**} eine reelle Zahl ist, ist E_i semiprimär, folglich auch reell. Hiedurch gelten die zu (21) konjugiert imaginären Gleichungen

$$\frac{\sigma_1^{**}+\sigma_2^{**}\zeta^{-i}}{1-\zeta^{-i}}=E_i \qquad (i=1,2,\ldots,p-1),$$

welche mit (21) die unmöglichen Gleichungen

$$(\sigma_1^{**}+\sigma_2^{**})(1+\zeta^{i})(1+\zeta^{-i})=0 \quad (i=1,2,\ldots,p-1)$$

ergeben. Damit ist unser Beweis vollzogen.

(Eingegangen am 16. November 1950.)